AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-63. (Cancelled)

64. (new) A method of storing a data set on a storage device carrying a file of random data comprising the steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for storing a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

65. (new) A method of operating a computer to store a data set on a storage device carrying a file of random data, the method comprising the steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

66. (new) A method according to claim 64 in which the step of selecting the first location for storing the file index comprises the step of selecting the first location as a start point of the file index.

67. (new) A method according to claim 64 in which the encrypted file index is stored directly at the first location.

68. (new) A method according to claim 64 in which the file index is stored at the first location in the file of random data by processing the random data using the encrypted file index.

69. (new) A method according to claim 64 in which the encrypted data is stored directly at the second location.

70. (new) A method according to claim 64 in which the data set is stored at the second selected location in the file of random data by processing the random data using the encrypted data set.

71. (new) A method according to claim 64 which comprises the step of using the user input passphrase for generating a key for encrypting the file index.

72. (new) A method according to claim 64 in which the passphrase is used for generating a key for encrypting the data set.

73. (new) A method according to claim 64 in which the passphrase is used in selecting the second location.

74. (new) A method according to claim 64 in which at least one of the first location, the second location, a key for the file index and a key for the data set is determined by using at least one hash function to operate on the user input passphrase.

75. (new) A method according to claim 64 in which the passphrase is operated on once to produce an output which is used for determining at least two of the first location, the second location, a key for the file index and a key for the data set.

76. (new) A method according to claim 64 in which the passphrase is operated on a plurality of times, each operation generating an output for use in determining at least one of the first location, the second location, a key for the file index and a key for the data set.

77. (new) A method according to claim 64 in which the same key is used for encrypting the set of data as is used for encrypting the file index.

78. (new) A method according to claim 64 which comprises the step of storing further sets of data using the same passphrase.

79. (new) A method according to claim 78 which is such that a respective location for each data set is selected, each data set is encrypted and stored at the respective location, and respective entries are added to the file index.

80. (new) A method according to claim 64, comprising the step of storing further file indexes within the file of random data, each of which indexes is associated with a respective passphrase and each of which indexes is encrypted and is stored at a location selected in dependence on the respective passphrase.

81. (new) A method according to claim 80 in which respective encryption keys are generated from the respective passphrases and these respective keys are used for encrypting data sets which are associated with each file index.

82. (new) A method according to claim 80 comprising the step of selecting the passphrase for, and hence location for, an additional file index in the knowledge of all of the existing passphrases corresponding to file indexes already stored in the file of random data such that collisions may be avoided.

83. (new) A method according to claim 80, in which, where there are a plurality of file indexes stored in the file of random data, the method comprises the step of selecting a location for an additional data set in the knowledge of all of the existing passphrases corresponding to file indexes already stored in the file of random data such that collisions may be avoided.

84. (new) A method according to claim 80 comprising the step of storing additional data sets using a passphrase whilst in ignorance of at least one other existing passphrase.

85. (new) A method according to claim 80 comprising the step of storing data sets in a predetermined relationship to the respective file index to help prevent collisions, for example data sets may be stored adjacent to the respective file index, data sets may be

stored substantially contiguously to the respective file index, and data sets may be stored at locations close to but after the respective file index.

86. (new) A method according to claim 64 comprising the step of storing data on a storage device carrying a plurality of files of random data.

87. (new) A method according to claim 64 in which the file index comprises a message authentication code.

88. (new) A method according to claim 87 in which the file index comprises a message authentication code of all associated data sets so as to facilitate the detection of tampering.

89. (new) A method according to claim 87 in which the file index comprises a message authentication code of the whole of the file of random data for use in detecting other usage of the file.

90. (new) A method according to claim 64 comprising the step of pre-processing the data set prior to encryption.

91. (new) A method according to claim 64 comprising the step of presenting a user with an indication of the location within the file of random data that will be selected for the file index when using a predetermined passphrase.

92. (new) A method according to claim 91 comprising the step of accepting user entered trial passphrases and providing the user with an indication of the location within the file of random data that will be selected for the file index for each trial passphrase.

93. (new) A method according to claim 91 comprising the further step of providing to the user an indication of the regions of the file of random data that are already occupied by file indexes having passphrases that have been supplied by the user.

94. (new) A method according to claim 64 comprising the step of receiving an indication from a user of a location within the file of random data which the user desires to use for a file index.

95. (new) A method according to claim 94 comprising the step of suggesting possible passphrases to a user in response to a user indicating a location within the file of random data which the user desires to use for a file index.

96. (new) A method according to claim 94 comprising the steps of receiving a user input passphrase and suggesting a modified passphrase.

97. (new) A method according to claim 96 in which the modification of the passphrase is selected so as to at least one of: move the location at which the associated index would be stored towards a desired location indicated by the user and strengthen the passphrase.

98. (new) A method according to claim 64 comprising the step of deleting a data set stored on a storage device.

99. (new) A method according to claim 98 comprising the step of removing the respective entry from the file index.

100. (new) A method according to claim 99 in which the deleting step comprises the step of overwriting the data set with random data as well as removing the entry from the file index.

101. (new) A method according to claim 98 comprising the step of reorganising data stored in association with a file index when at least one data set referenced in that file index is deleted.

102. (new) A method according to claim 100 in which the overwriting step comprises the step of using at least one random data and encrypted data stored in the file of random data for generating pseudo-random data for overwriting deleted files.

103. (new) A method according to claim 102 in which the method comprises the step of using random numbers from the file of random data that would be overwritten when adding a data set to replace any pseudo-random values previously used elsewhere within the file of random data.

104. (new) A storage device carrying a file of random data in which file of random data is stored a file index and a data set, wherein the file index is encrypted and is stored at a first location determined by a passphrase, the data set is encrypted and is stored at a second location and the file index comprises an entry in respect of the data set, the entry comprising an indication of the second location.

105. (new) A storage device according to claim 104 carrying software for use in the storing and extraction of data sets in the random data.

106. (new) A storage device according to claim 104 in which the passphrase has been used to generate a key for at least one of encrypting the file index and encrypting the data set.

107. (new) A storage device according to claim 104 in which the software carried by the storage device is arranged such that when loaded and run by a computer, the computer is caused to carry out at least one of the following steps:

accepting passphrases, generating corresponding keys, and determining respective locations for storage of file indexes;

encrypting file indexes;

encrypting data sets;

storing file indexes;

selecting locations for data sets;

storing data sets;

accepting passphrases and locating and decrypting respective file indexes;

locating and decrypting data sets;

retrieving data sets.

108. (new) A storage device according to claim 104 which further carries a conventional file allocation table.

109. (new) A storage device according to claim 104 which comprises a portion of Read Only Memory (ROM).

110. (new) A storage device according to claim 108 which comprises a ROM portion that carries the file allocation table, the software and an operating system header file for the file of random data.

111. (new) The storage device according to claim 104 which is a removable storage device.

112. (new) A storage device according to claim 104 having a unique serial number.

113. (new) A storage device according to claim 104 which carries a unique hard coded identifier which is used in at least one of the encryption and decryption process.

114. (new) A storage device according to claim 104 which is sold with a pretext for at least one use.

115. (new) A computer arranged under the control of software for storing a data set on a storage device carrying a file of random data using the steps of:
selecting, in dependence on a user input passphrase, a first location within the file of random data for the storing a file index;
selecting a second location within the file of random data for storing the data set;
encrypting the data set;
storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

116. (new) A computer according to claim 115 which is arranged under the control of software to present a user with an indication of the location within the file of random data that will be selected for storing the file index when using a predetermined passphrase.

117. (new) A computer according to claim 115 which is arranged under the control of software to accept user entered trial passphrases and provide the user with an indication of the location within the file of random data that will be selected for storing the file index for each trial passphrase.

118. (new) A computer according to claim 115 which is arranged under the control of software to provide the user an indication of the regions of the file of random data that are already occupied by file indexes having passphrases that have been supplied by the user.

119. (new) A computer according to claim 115 which is arranged under the control of software to suggest possible passphrases to a user in response to a user indicating a

location within the file of random data which the user desires to use for storing a file index.

120. (new) A computer according to claim 116 which is arranged under the control of software to present a user interface for displaying the indications.

121. (new) A computer according to claim 120 in which the user interface is arranged so that a user can use a pointing device to indicate the location within the file of random data which the user desires to use for storing a file index.

122. (new) A method of extracting a data set stored on a storage device according to claim 104, the method of extracting data comprising the steps of:
accepting a user input passphrase;
determining the location for a file index indicated by the passphrase;
decrypting the file index;
identifying the location of the requested data set from the file index; and
decrypting the data set.

123. (new) A computer arranged under the control of software to extract data using a method according to claim 122.

124. (new) A method of storing a data set on a storage device carrying a file of random data comprising the steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for storing a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising a indication of the second selected location;

encrypting the file index; and

storing the file index at the first selected location in the file of random data, wherein the method comprises the further steps, prior to finalising the user input passphrase, of accepting at least one user entered trial passphrase and providing the user with an indication of the location within the file of random data that will be selected for the file index associated with the at least one user entered trial passphrase.

125. (new) A computer readable data carrier, carrying a computer program comprising code portions which when loaded and run on a computer cause the computer to carry out a method according to claim 64.